DEPARTMENT OF THE NAVY
PROGRAM EXECUTIVE OFFICER, SUBMARINES
614 SICARD STREET SE
WASHINGTON NAVY YARD DC 20376-7004

IN REPLY TO

2070
Ser TSUB/111
19 May 04

From: Program Executive Officer (Submarines)

Subj: POLICY REGARDING REGISTRATION, CERTIFICATION AND
        ACCREDITATION OF INFORMATION TECHNOLOGY SYSTEMS AND
        APPLICATIONS

Ref: (a) Federal Information Security Management Act (FISMA)
            of 2002
        (b) DoD Instruction 5000.2 of 12 May 03, "Operation of
            the Defense Acquisition System"
        (c) Interim Defense Acquisition Guidebook of 30 Oct 02
        (d) OSD Memorandum of 08 March 02, "Clinger-Cohen Act
            Compliance Policy"
        (e) OPNAVINST 5239.1B of 09 Nov 99, "Navy Information
            Assurance Program"
        (f) DoD Instruction 5200.40 of 01 Nov 99, "DoD
            Information Technology Security Certification
            and Accreditation (C&A) Process (DITSCAP)"
        (g) Director of Central Intelligence Directive (DCID
            6/3) of June 1999, "Protecting Sensitive
            Compartmented Information Within Information Systems"
        (h) Department of Defense Directive, of 24 October 2002,
            Numbered 8500.1, ASD(C3I), Information Assurance
            (IA)
        (i) NAVSEA Ltr Ser 00I/310 of 24 Feb 03, "Developmental
            Designated Approving Authority (DDAA) Appointment"
        (j) OPNAV NOTE 5230, Ser DNS/3U501808 of 3 Aug 03,
            "Appointment of Designated Approving Authority (DAA)
            For All Operational Navy Information Technology (IT)
            Systems and Networks

1. Purpose. The purpose of this memorandum is to establish an
Information Assurance (IA) Policy and Process for Information
Technology (IT) business and National Security Systems (NSS)
under the cognizance of the Program Executive Officer for
Submarines (PEO SUB) and SEA 07. This memorandum disseminates
policy and guidance concerning IT requirements related to
Clinger-Cohen Act (CCA) compliance, as well as certification and
accreditation (C&A) documentation, DON CIO registration and the
coordination of Information Assurance Vulnerabilities Alert
(IAVA) policy compliance for tactical and weapons systems of PEO
SUB IT systems and applications.

Subj: POLICY REGARDING REGISTRATION, CERTIFICATION AND
ACCREDITATION OF INFORMATION TECHNOLOGY SYSTEMS AND
APPLICATIONS

2. Background. The proliferation of IT in national security
and business systems, combined with current DoD and DON
initiatives to consolidate IT systems and to safeguard
information from unauthorized access has resulted in significant
changes in the acquisition process as reflected in the
requirements of references (a) through (j). Driven primarily by
the Clinger-Cohen Act of 1996, systems utilizing IT must be
registered in a DoD-wide database referred to as the DoD IT
Registry. During all acquisition phases, each system must
demonstrate that it meets the requirements of reference (d). To
ensure safe and secure operation, each system's IT-related
capabilities are to be certified by the Developmental Designated
Approval Authority (DDAA) for tactical and weapon systems, or
the Designated Approval Authority (DAA) for business systems as
applicable, in accordance with references (i) and (j).

3. Scope. This policy applies to all PEO SUB acquisition
programs that contain and utilize IT to digitally process data.
Additionally, this policy applies to all business-related IT
systems, including applications, web sites, and other internal
tools utilized to execute the PEO SUB and SEA 07 missions,
whether sponsored, funded, or owned by TEAM SUB organizations.

4. Policy. All IT systems must meet all requirements
established in references (a) through (j) as well as other
applicable DoD, DoN, and NAVSEA requirements contained in
governing documents not directly referenced in this policy. All
PEO SUB IT systems and applications shall be registered in the
DON CIO IT Registration Database that uploads into the DoD IT
Registry. For tactical and weapon systems, the DDAA shall
provide the ACIO with completed documents at each milestone in
the DITSCAP C&A process. The ACIO is designated as the PEO SUB
representative to assist Program Managers in determining the
exact requirements that apply to business-related IT systems.
The PEO SUB DDAA is designated as the PEO SUB representative to
assist Program Managers in determining the exact requirements
that apply to tactical and weapon systems. Where it is unclear
if a system should be considered a business or National Security
System (NSS), the ACIO and DDAA will work together to determine
and ensure the appropriate level of compliance for the system
when it crosses business and NSS boundaries.

Subj: POLICY REGARDING REGISTRATION, CERTIFICATION AND
        ACCREDITATION OF INFORMATION TECHNOLOGY SYSTEMS AND
        APPLICATIONS

5.   Roles and Responsibilities.   The following roles and
responsibilities are assigned:

(a) PEO SUB has delegated Developmental Designated Approval
Authority (DDAA) for all PEO SUB tactical and weapon systems to
the PEO SUB Warfare Chief Systems Engineer (SUB-W) for submarine
acquisition programs. The DDAA is responsible for all
Information Assurance (IA) IT policies, processes, and
procedures within PEO SUB to ensure submarine tactical and
weapon system-related information resources are secure and
protected. The DDAA will facilitate DoD Intelligence
Information System (DoDIIS) compliance where required in
accordance with reference (g). The DDAA will collaborate with
the ACIO to disseminate integrated and comprehensive PEO SUB IA
processes and to educate all personnel on their roles and
responsibilities. In accordance with reference (i), the DDAA
will approve C&A and coordinate with the appropriate operational
DAA to ensure an IATO/ATO is in place prior to land based or
shipboard operation of tactical and weapon systems under PEO SUB
cognizance. The DDAA will coordinate efforts for IAVA policy for
developmental and fielded submarine tactical and weapon system-
related information resources with the appropriate IAVA
designated authorities.

(b) The Activity Command Information Officer (ACIO) is
responsible for all IA IT policies, processes, and procedures
within PEO SUB to ensure business-related information resources
are secure and protected. In accordance with ref (i), the ACIO
will work with the NAVSEA CIO and the appropriate operational
DAA to ensure that business-related information systems are
certified and accredited for security purposes. The ACIO will
provide access to a single data source of all required
documentation for IT systems and applications to the operational
DAA, NETWARCOM, for all C&A milestone approvals and milestone
documents, all Authority to Operate (ATO), Interim Authority to
Operate (IATO), waiver letters and supporting documentation.

(c) Program Managers (PMs) are responsible to ensure that IT
systems under their cognizance receive certification and
accreditation in a timely manner in accordance with the PEO SUB
IA policy and processes, shall endorse all System Security
Authorization Agreements (SSAAs) prior to submission, and ensure
compliance with IAVAs for their program of record.

Subj: POLICY REGARDING REGISTRATION, CERTIFICATION AND
       ACCREDITATION OF INFORMATION TECHNOLOGY SYSTEMS AND
       APPLICATIONS

6.   The PEO SUB point of contact for guidance in complying with
CCA requirements, IT Registration, and C&A of business-related
information systems and applications and all C&A milestone
documentation is the ACIO, Ms. Claudia Linnens. The PEO SUB
point of contact for guidance in complying with CCA
requirements, IT registration, and and C&A of submarine tactical
and weapon systems is the DDAA, Mr. Jim Thompson.

J. D. BUTLER
Rear Admiral, U.S. Navy

Distribution:
DON CIO
N61
N77
N776
NETWARCOM
COMSUBLANT N6
COMSUBPAC N6
NAVSEA CIO
NUWC 00
NUWC CIO
NSWC CIO

Copy to:
All Team Sub Offices
TEAM SUB ACIO
TEAM SUB AO